PCT/JP99/00292

日本国特許庁

PATENT OFFICE
JAPANESE GOVERNMENT

09/381996 PCT

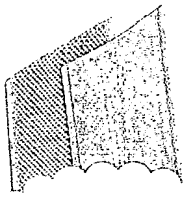
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９８年　２月　９日

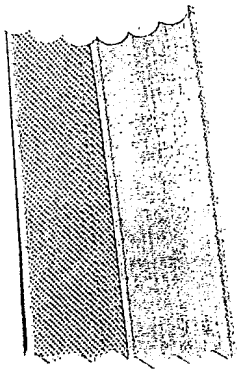
出願番号
Application Number: 平成１０年特許願第０２７５７２号

出願人
Applicant (s): 松下電器産業株式会社



PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)



１９９９年　３月２６日

特許庁長官
Commissioner,
Patent Office 伴佐山建志

出証番号　出証特平１１－３０１７３９３

【書類名】　特許願

【整理番号】　2054500013

【提出日】　平成10年 2月 9日

【あて先】　特許庁長官殿

【国際特許分類】　G11B 20/00

【発明の名称】　録画装置および再生装置

【請求項の数】　27

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　山田　正純

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　飯塚　裕之

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　武知　秀明

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　後藤　昌一

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100092794

【弁理士】

出証特平１１－３０１７３９３

【氏名又は名称】　松田　正道

【電話番号】　06 397-2840

【手数料の表示】

【予納台帳番号】　009896

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9006027

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　録画装置および再生装置

【特許請求の範囲】

【請求項１】映像および／または音のデータを入力するとともに、前記映像および／または音のデータをスクランブルするためのスクランブル鍵を入力し、そのスクランブル鍵で前記映像および／または音のデータをスクランブルするスクランブル手段と、

前記スクランブル鍵を暗号化するための暗号化鍵を発生する暗号化鍵発生手段と、

前記暗号化鍵発生手段が発生した暗号化鍵を格納し、その後、その暗号化鍵が所定の条件に合えば、その暗号化鍵を消去する格納手段と、

前記スクランブル手段からのスクランブル鍵を入力するとともに、前記暗号化鍵発生手段からの前記暗号化鍵を入力し、その暗号化鍵で前記スクランブル鍵を暗号化する鍵暗号化手段と、

前記スクランブル鍵によりスクランブルされた映像および／または音のデータと、そのスクランブル鍵を暗号化した暗号化鍵との対応関係情報を生成する対応関係情報生成手段と、

前記スクランブル手段からのスクランブルされた映像および／または音のデータ、前記鍵暗号化手段からの暗号化されたスクランブル鍵、および、前記対応関係情報生成手段からの対応関係情報の全部または一部を入力し、それらを所定の記録媒体に記録する記録手段とを

備えたことを特徴とする録画装置。

【請求項２】前記所定の条件とは、前記暗号化鍵が格納された後、所定の時間を超えることを意味することを特徴とする請求項１記載の録画装置。

【請求項３】前記対応関係情報とは、前記スクランブル手段が前記映像および／または音のデータを入力した日時、前記スクランブル手段が前記スクランブル鍵で前記映像および／または音のデータをスクランブルした日時、前記暗号化鍵発生手段が前記暗号化鍵を発生した日時、前記格納手段が前記暗号化鍵を格納した日時、前記鍵暗号化手段が前記暗号化鍵で前記スクランブル鍵を暗号化した日

出証特平１１－３０１７３９３

時、または、前記記録手段が前記所定の記録媒体に前記スクランブルされた映像および／または音のデータを記録した日時で対応付けられた情報であることを特徴とする請求項１または２記載の録画装置。

【請求項４】前記所定の条件とは、前記スクランブルされた映像および／または音のデータの再生のさいに、前記暗号化鍵の利用された回数が、所定の回数を超えることを意味することを特徴とする請求項１記載の録画装置。

【請求項５】前記スクランブル鍵を発生するスクランブル鍵発生手段を備え、前記スクランブル手段は、前記スクランブル鍵発生手段から前記スクランブル鍵を入力することを特徴とする請求項１から４のいずれかに記載の録画装置。

【請求項６】前記スクランブル手段は、放送局からの前記スクランブル鍵を入力し、そのスクランブル鍵を利用することを特徴とする請求項１から４のいずれかに記載の録画装置。

【請求項７】請求項１から６のいずれかに記載の所定の記録媒体からの、請求項１から６のいずれかに記載の前記対応関係情報を入力し、その対応関係情報に基づいて、再生しようとするスクランブルされた映像および／または音のデータに対応する暗号化鍵を特定し、請求項１から６のいずれかに記載の格納手段のなかの前記暗号化鍵を検索して取得する暗号化鍵取得手段と、

前記所定の記録媒体からの、前記再生しようとするスクランブルされた映像および／または音のデータに対応する、暗号化されたスクランブル鍵を入力するとともに、前記暗号化鍵取得手段からの暗号化鍵を入力し、その暗号化鍵で前記暗号化された前記スクランブル鍵の暗号化を解く鍵暗号化解読手段と、

前記所定の記録媒体からの、スクランブルされた映像および／または音のデータを入力するとともに、前記鍵暗号化解読手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記スクランブルされた映像および／または音のデータのスクランブルを解除するスクランブル解除手段とを

備えたことを特徴とする再生装置。

【請求項８】映像および／または音のデータを入力するとともに、前記映像および／または音のデータをスクランブルするためのスクランブル鍵を入力し、そのスクランブル鍵で前記映像および／または音のデータをスクランブルするスク

ランブル手段と、

前記スクランブル鍵を暗号化するための暗号化鍵を発生する暗号化鍵発生手段と、

前記暗号化鍵発生手段が発生した暗号化鍵を格納する格納手段と、

前記スクランブル手段からのスクランブル鍵を入力するとともに、前記暗号化鍵発生手段からの前記暗号化鍵を入力し、その暗号化鍵で前記スクランブル鍵を暗号化する鍵暗号化手段と、

前記スクランブル鍵によりスクランブルされた映像および／または音のデータと、そのスクランブル鍵を暗号化した暗号化鍵との対応関係情報を生成する対応関係情報生成手段と、

前記スクランブル手段からのスクランブルされた映像および／または音のデータ、前記鍵暗号化手段からの暗号化されたスクランブル鍵、および、前記対応関係情報生成手段からの対応関係情報の全部または一部を入力し、それらを所定の記録媒体に記録する記録手段とを

備えたことを特徴とする録画装置。

【請求項９】前記対応関係情報とは、前記スクランブル手段が前記映像および／または音のデータを入力した日時、前記スクランブル手段が前記スクランブル鍵で前記映像および／または音のデータをスクランブルした日時、前記暗号化鍵発生手段が前記暗号化鍵を発生した日時、前記格納手段が前記暗号化鍵を格納した日時、前記鍵暗号化手段が前記暗号化鍵で前記スクランブル鍵を暗号化した日時、または、前記記録手段が前記所定の記録媒体に前記スクランブルされた映像および／または音のデータを記録した日時で対応付けられた情報であることを特徴とする請求項８記載の録画装置。

【請求項１０】前記スクランブル鍵を発生するスクランブル鍵発生手段を備え、前記スクランブル手段は、前記スクランブル鍵発生手段から前記スクランブル鍵を入力することを特徴とする請求項８または９記載の録画装置。

【請求項１１】前記スクランブル手段は、放送局からの前記スクランブル鍵を入力し、そのスクランブル鍵を利用することを特徴とする請求項８または９記載の録画装置。

【請求項１２】請求項８から１１のいずれかに記載の所定の記録媒体からの、請求項８から１１のいずれかに記載の対応関係情報を入力し、その対応関係情報に基づいて、再生しようとするスクランブルされた映像および／または音のデータに対応する暗号化鍵を特定し、さらに、その暗号化鍵が所定の条件に合うかどうかを判定し、合致する場合は、その暗号化鍵を、請求項８から１１のいずれかに記載の格納手段から取り出し、合致しない場合は、その暗号化鍵を前記格納手段から取り出さない暗号化鍵取得手段と、

前記所定の記録媒体からの、前記再生しようとするスクランブルされた映像および／または音のデータに対応する、暗号化されたスクランブル鍵を入力するとともに、前記暗号化鍵取得手段からの暗号化鍵を入力し、その暗号化鍵で前記暗号化された前記スクランブル鍵の暗号化を解く鍵暗号化解読手段と、

前記所定の記録媒体からの、スクランブルされた映像および／または音のデータを入力するとともに、前記鍵暗号化解読手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記スクランブルされた映像および／または音のデータのスクランブルを解除するスクランブル解除手段とを

備えたことを特徴とする再生装置。

【請求項１３】前記所定の条件とは、請求項８から１１のいずれかに記載の格納手段に、前記暗号化鍵が格納された後、所定の時間を超えることを意味することを特徴とする請求項１２記載の再生装置。

【請求項１４】前記所定の条件とは、前記スクランブルされた映像および／または音のデータの再生のさいに、前記暗号化鍵の利用された回数が、所定の回数を超えることを意味することを特徴とする請求項１２記載の再生装置。

【請求項１５】映像および／または音のデータをスクランブルするためのスクランブル鍵を発生するスクランブル鍵発生手段と、

前記スクランブル鍵発生手段が発生したスクランブル鍵を格納し、その後、そのスクランブル鍵が所定の条件に合えば、そのスクランブル鍵を消去する格納手段と、

前記映像および／または音のデータを入力するとともに、前記スクランブル鍵発生手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記映像および

／または音のデータをスクランブルするスクランブル手段と、

前記スクランブル鍵によりスクランブルされた映像および／または音のデータと、そのスクランブル鍵との対応関係情報を生成する対応関係情報生成手段と、

前記スクランブル手段からのスクランブルされた映像および／または音のデータ、および、前記対応関係情報生成手段からの対応関係情報の全部または一部を入力し、それらを所定の記録媒体に記録する記録手段とを

備えたことを特徴とする録画装置。

【請求項１６】前記所定の条件とは、前記スクランブル鍵が格納された後、所定の時間を超えることを意味することを特徴とする請求項１５記載の録画装置。

【請求項１７】前記対応関係情報とは、前記スクランブル手段が前記映像および／または音のデータを入力した日時、前記スクランブル手段が前記スクランブル鍵で前記映像および／または音のデータをスクランブルした日時、前記スクランブル鍵発生手段が前記スクランブル鍵を発生した日時、前記格納手段が前記スクランブル鍵を格納した日時、または、前記記録手段が前記所定の記録媒体に前記スクランブルされた映像および／または音のデータを記録した日時で対応付けられた情報であることを特徴とする請求項１５または１６記載の録画装置。

【請求項１８】前記所定の条件とは、前記スクランブルされた映像および／または音のデータの再生のさいに、前記暗号化鍵の利用された回数が、所定の回数を超えることを意味することを特徴とする請求項１５記載の録画装置。

【請求項１９】請求項１５から１８のいずれかに記載の所定の記録媒体からの、請求項１５から１８のいずれかに記載の対応関係情報を入力し、その対応関係情報に基づいて、再生しようとするスクランブルされた映像および／または音のデータに対応するスクランブル鍵を特定し、請求項１５から１８のいずれかに記載の格納手段のなかの前記スクランブル鍵を検索して取得するスクランブル鍵取得手段と、

前記所定の記録媒体からの、前記再生しようとするスクランブルされた映像および／または音のデータに対応する、前記スクランブルされた映像および／または音のデータを入力するとともに、前記スクランブル鍵取得手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記スクランブルされた映像および／ま

たは音のデータのスクランブルを解除するスクランブル解除手段とを

備えたことを特徴とする再生装置。

【請求項２０】映像および／または音のデータをスクランブルするためのスクランブル鍵を発生するスクランブル鍵発生手段と、

前記スクランブル鍵発生手段が発生したスクランブル鍵を格納する格納手段と、

前記映像および／または音のデータを入力するとともに、前記スクランブル鍵発生手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記映像および／または音のデータをスクランブルするスクランブル手段と、

前記スクランブル鍵によりスクランブルされた映像および／または音のデータと、そのスクランブル鍵との対応関係情報を生成する対応関係情報生成手段と、

前記スクランブル手段からのスクランブルされた映像および／または音のデータ、および、前記対応関係情報生成手段からの対応関係情報の全部または一部を入力し、それらを所定の記録媒体に記録する記録手段とを

備えたことを特徴とする録画装置。

【請求項２１】前記対応関係情報とは、前記スクランブル手段が前記映像および／または音のデータを入力した日時、前記スクランブル手段が前記スクランブル鍵で前記映像および／または音のデータをスクランブルした日時、前記スクランブル鍵発生手段が前記スクランブル鍵を発生した日時、前記格納手段が前記スクランブル鍵を格納した日時、または、前記記録手段が前記所定の記録媒体に前記スクランブルされた映像および／または音のデータを記録した日時で対応付けられた情報であることを特徴とする請求項２０記載の録画装置。

【請求項２２】請求項２０または２１記載の所定の記録媒体からの、請求項２０または２１記載の対応関係情報を入力し、その対応関係情報に基づいて、再生しようとするスクランブルされた映像および／または音のデータに対応するスクランブル鍵を特定し、さらに、そのスクランブル鍵が所定の条件に合うかどうかを判定し、合致する場合は、そのスクランブル鍵を、請求項２０または２１記載の格納手段から取り出し、合致しない場合は、そのスクランブル鍵を前記格納手段から取り出さないスクランブル鍵取得手段と、

前記所定の記録媒体からの、前記再生しようとするスクランブルされた映像および／または音のデータに対応する、スクランブルされた映像および／または音のデータを入力するとともに、前記スクランブル鍵取得手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記スクランブルされた映像および／または音のデータのスクランブルを解除するスクランブル解除手段とを

備えたことを特徴とする再生装置。

【請求項２３】前記所定の条件とは、請求項２０または２１記載の格納手段に、前記スクランブル鍵が格納された後、所定の時間を超えることを意味することを特徴とする請求項２２記載の再生装置。

【請求項２４】前記所定の条件とは、前記スクランブルされた映像および／または音のデータの再生のさいに、前記スクランブル鍵の利用された回数が、所定の回数を超えることを意味することを特徴とする請求項２２記載の再生装置。

【請求項２５】前記記録手段が前記スクランブル手段からのスクランブルされた映像および／または音のデータを、前記所定の記録媒体に記録するさい、前記データの記録に対する課金を課す課金手段を備えたことを特徴とする請求項１から６のいずれか、または、請求項８から１１のいずれか、または、請求項１５から１８のいずれか、または、請求項２０から２１のいずれかに記載の録画装置。

【請求項２６】前記所定の記録媒体は、ビデオテープであることを特徴とする請求項１から６のいずれか、または、請求項８から１１のいずれか、または、請求項１５から１８のいずれか、または、請求項２０から２１のいずれかに記載の録画装置。

【請求項２７】前記所定の記録媒体は、ハードディスクであることを特徴とする請求項１から６のいずれか、または、請求項８から１１のいずれか、または、請求項１５から１８のいずれか、または、請求項２０から２１のいずれかに記載の録画装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、著作権等により再生についての期間や回数が制限された、映像およ

び／または音のデータを録画する録画装置と、その映像および／または音のデータを再生する再生装置とに関するものである。

【０００２】

【従来の技術】

現在、著作権保護の対象となっている映画や音楽等のＡＶデータは、ビデオテープ等に格納されている。ユーザは、そのようなビデオテープ等を有料で貸し出すレンタル店を通じて、例えば１週間というような所定の期間のみビデオテープ等を借り、それを再生することによって、映画や音楽等を鑑賞することができる。

【０００３】

他方、上述したビデオテープ等のレンタルのシステムとは別に、ディジタル技術や暗号化技術の進歩等から、放送局からの映画や音楽等の番組を通信衛星を介して入力し、その番組をスクランブルしてビデオテープ等に録画し、再生する録画再生装置として、以下のものが考えられている。

【０００４】

図７に、このような従来の録画再生装置のブロック図を示す。

【０００５】

受信復調手段１は、衛星放送の、デジィタルの映像データ、音データ、ＥＭＭ（個別情報）、ＥＣＭ（番組情報）および暗号化された放送スクランブル鍵Ｋｓを入力し、第１ＤＭＵＸ２は、受信復調手段１からの映像データ、音データ、ＥＭＭ、ＥＣＭおよび放送スクランブル鍵Ｋｓを分離する。そして、ＥＭＭ解読手段３は、第１ＤＭＵＸ２からのＥＭＭを入力するとともに、ユーザＩＤ鍵Ｋｍを入力し、そのユーザＩＤ鍵ＫｍでＥＭＭを解読してワーク鍵Ｋｗを生成する。ＥＣＭ解読手段４は、ＥＭＭ解読手段３からのワーク鍵Ｋｗを入力するとともに、第１ＤＭＵＸ２からのＥＣＭおよび暗号化された放送スクランブル鍵Ｋｓを入力し、ワーク鍵ＫｗでＥＣＭを解読して、暗号化された放送スクランブル鍵Ｋｓを復元する。

【０００６】

その後、放送デスクランブル手段５は、ＥＣＭ解読手段４からの放送スクラン

ブル鍵Ｋｓを入力するとともに、第１ＤＭＵＸ２からの、スクランブルされたＡＶデータを入力し、放送スクランブル鍵Ｋｓで、スクランブルされたＡＶデータをデスクランブルする。そして、放送デスクランブル手段５は、デスクランブルされたＡＶデータを、リアルタイムでＡＶデータを直接ディスプレイ２１に表示させる場合に第１ＤＭＵＸ２に出力し、また、ビデオテープ２０にＡＶデータを記録させる場合に記録スクランブル手段７に出力する。

【０００７】

放送デスクランブル手段５がＡＶデータを第１ＤＭＵＸ２に出力する場合、第１ＤＭＵＸ２は、放送デスクランブル手段５からのＡＶデータを映像データと音データに分離して、映像データを映像デコーダ１８に出力し、音データを音デコーダ１９に出力する。そして、映像デコーダ１８および音デコーダ１９それぞれは、第１ＤＭＵＸ２からの映像データまたは音データを復号し、ディスプレイ２１は、映像を表示し音を出力する。

【０００８】

他方、放送デスクランブル手段５がＡＶデータを記録スクランブル手段７に出力する場合、記録スクランブル手段７は、放送デスクランブル手段５からのＡＶデータを入力するとともに、第１鍵発生手段６からの記録スクランブル鍵Ｋｓｓを入力し、その記録スクランブル鍵Ｋｓｓで、ＡＶデータをスクランブルする。その記録スクランブル鍵Ｋｓｓによりスクランブルされたデータを{Ｋｓｓ（ＡＶデータ）}とする。

【０００９】

それとともに、第２鍵発生手段８は、記録スクランブル鍵Ｋｓｓを暗号化するための暗号化鍵Ｋｃを発生し、鍵暗号化手段１０は、第１鍵発生手段６からの記録スクランブル鍵Ｋｓｓを入力するとともに、第２鍵発生手段８からの暗号化鍵Ｋｃを入力し、その暗号化鍵Ｋｃで記録スクランブル鍵Ｋｓｓを暗号化する。その暗号化鍵Ｋｃにより暗号化された記録スクランブル鍵Ｋｓｓを{Ｋｃ（Ｋｓｓ）}とする。

【００１０】

そして、ＭＵＸ１２は、記録スクランブル手段７からの{Ｋｓｓ（ＡＶデータ）}

と、鍵暗号化手段１０からのＫｃ（Ｋｓｓ）とを入力し、それらをビデオテープ２０に記録する。

【００１１】

そのビデオテープ２０に記録されたＫｓｓ（ＡＶデータ）を再生する場合、先ず、第２ＤＭＵＸ１３は、ビデオテープ２０からのＫｓｓ（ＡＶデータ）と、Ｋｃ（Ｋｓｓ）とを入力して分離する。そして、鍵解読手段１６は、第２ＤＭＵＸ１３からのＫｃ（Ｋｓｓ）を入力するとともに、第２鍵発生手段８からの暗号化鍵Ｋｃを入力し、その暗号化鍵ＫｃでＫｃ（Ｋｓｓ）を解読して、記録スクランブル鍵Ｋｓｓを復元する。さらに、再生デスクランブル手段１７は、第２ＤＭＵＸ１３からのＫｓｓ（ＡＶデータ）を入力するとともに、鍵解読手段１６からの記録スクランブル鍵Ｋｓｓを入力し、その記録スクランブル鍵ＫｓｓでＫｓｓ（ＡＶデータ）をデスクランブルして、そのデスクランブルされたＡＶデータを第１ＤＭＵＸ２に出力する。

【００１２】

最後に、第１ＤＭＵＸ２に出力されたＡＶデータは、リアルタイムにおける、ディスプレイ２１の映像表示および音出力と同様にして、ディスプレイ２１によって映像として表示され、また、音として出力される。

【００１３】

【発明が解決しようとする課題】

ところで、上述したビデオテープ等のレンタルのシステムは、これからの多チャンネルディジタル放送時代においても、ユーザがその都度レンタル店に出向いてビデオテープ等を借りなければならないという点など、ユーザにとって相変わらず手間がかかり不便である。

【００１４】

また、上述した従来の録画再生装置では、ＡＶデータを一度ビデオテープ２０に記録すると、第２鍵発生手段８からの暗号化鍵Ｋｃを利用しさえすれば、そのＡＶデータは、いつでも、また、何度でも再生され、ディスプレイ２１によって映像および／または音として出力される。このように、従来の録画再生装置では、映画や音楽等の著作権保護の対象となっているＡＶデータの有効再生期間や有

効再生回数には制限がないということになる。例えば、劇場放映直後の映画のように、特別な価値を有するＡＶデータが上述したような、再生の期間や回数について制限のない録画再生装置によって記録媒体に記録されると、そのＡＶデータの価値は半減する。つまり、放送局は、そのような特別な価値を有するＡＶデータを安心して放送することができない。

【００１５】

本発明は、このような従来の録画再生装置は、ＡＶデータを記録媒体に記録すると、そのＡＶデータの有効再生期間や有効再生回数の制限を守らないという課題を考慮し、ＡＶデータを記録媒体に記録し、そのＡＶデータの有効再生期間や有効再生回数の制限を遵守する録画装置および再生装置を提供することを目的とするものである。

【００１６】

【課題を解決するための手段】

請求項１の本発明は、映像および／または音のデータを入力するとともに、前記映像および／または音のデータをスクランブルするためのスクランブル鍵を入力し、そのスクランブル鍵で前記映像および／または音のデータをスクランブルするスクランブル手段と、前記スクランブル鍵を暗号化するための暗号化鍵を発生する暗号化鍵発生手段と、前記暗号化鍵発生手段が発生した暗号化鍵を格納し、その後、その暗号化鍵が所定の条件に合えば、その暗号化鍵を消去する格納手段と、前記スクランブル手段からのスクランブル鍵を入力するとともに、前記暗号化鍵発生手段からの前記暗号化鍵を入力し、その暗号化鍵で前記スクランブル鍵を暗号化する鍵暗号化手段と、前記スクランブル鍵によりスクランブルされた映像および／または音のデータと、そのスクランブル鍵を暗号化した暗号化鍵との対応関係情報を生成する対応関係情報生成手段と、前記スクランブル手段からのスクランブルされた映像および／または音のデータ、前記鍵暗号化手段からの暗号化されたスクランブル鍵、および、前記対応関係情報生成手段からの対応関係情報の全部または一部を入力し、それらを所定の記録媒体に記録する記録手段とを備えたことを特徴とする録画装置である。

【００１７】

請求項７の本発明は、請求項１から６のいずれかに記載の所定の記録媒体からの、請求項１から６のいずれかに記載の前記対応関係情報を入力し、その対応関係情報に基づいて、再生しようとするスクランブルされた映像および／または音のデータに対応する暗号化鍵を特定し、請求項１から６のいずれかに記載の格納手段のなかの前記暗号化鍵を検索して取得する暗号化鍵取得手段と、前記所定の記録媒体からの、前記再生しようとするスクランブルされた映像および／または音のデータに対応する、暗号化されたスクランブル鍵を入力するとともに、前記暗号化鍵取得手段からの暗号化鍵を入力し、その暗号化鍵で前記暗号化された前記スクランブル鍵の暗号化を解く鍵暗号化解読手段と、前記所定の記録媒体からの、スクランブルされた映像および／または音のデータを入力するとともに、前記鍵暗号化解読手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記スクランブルされた映像および／または音のデータのスクランブルを解除するスクランブル解除手段とを備えたことを特徴とする再生装置である。

【００１８】

請求項８の本発明は、映像および／または音のデータを入力するとともに、前記映像および／または音のデータをスクランブルするためのスクランブル鍵を入力し、そのスクランブル鍵で前記映像および／または音のデータをスクランブルするスクランブル手段と、前記スクランブル鍵を暗号化するための暗号化鍵を発生する暗号化鍵発生手段と、前記暗号化鍵発生手段が発生した暗号化鍵を格納する格納手段と、前記スクランブル手段からのスクランブル鍵を入力するとともに、前記暗号化鍵発生手段からの前記暗号化鍵を入力し、その暗号化鍵で前記スクランブル鍵を暗号化する鍵暗号化手段と、前記スクランブル鍵によりスクランブルされた映像および／または音のデータと、そのスクランブル鍵を暗号化した暗号化鍵との対応関係情報を生成する対応関係情報生成手段と、前記スクランブル手段からのスクランブルされた映像および／または音のデータ、前記鍵暗号化手段からの暗号化されたスクランブル鍵、および、前記対応関係情報生成手段からの対応関係情報の全部または一部を入力し、それらを所定の記録媒体に記録する記録手段とを備えたことを特徴とする録画装置である。

【００１９】

請求項１２の本発明は、請求項８から１１のいずれかに記載の所定の記録媒体からの、請求項８から１１のいずれかに記載の対応関係情報を入力し、その対応関係情報に基づいて、再生しようとするスクランブルされた映像および／または音のデータに対応する暗号化鍵を特定し、さらに、その暗号化鍵が所定の条件に合うかどうかを判定し、合致する場合は、その暗号化鍵を、請求項８から１１のいずれかに記載の格納手段から取り出し、合致しない場合は、その暗号化鍵を前記格納手段から取り出さない暗号化鍵取得手段と、前記所定の記録媒体からの、前記再生しようとするスクランブルされた映像および／または音のデータに対応する、暗号化されたスクランブル鍵を入力するとともに、前記暗号化鍵取得手段からの暗号化鍵を入力し、その暗号化鍵で前記暗号化された前記スクランブル鍵の暗号化を解く鍵暗号化解読手段と、前記所定の記録媒体からの、スクランブルされた映像および／または音のデータを入力するとともに、前記鍵暗号化解読手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記スクランブルされた映像および／または音のデータのスクランブルを解除するスクランブル解除手段とを備えたことを特徴とする再生装置である。

【００２０】

請求項１５の本発明は、映像および／または音のデータをスクランブルするためのスクランブル鍵を発生するスクランブル鍵発生手段と、前記スクランブル鍵発生手段が発生したスクランブル鍵を格納し、その後、そのスクランブル鍵が所定の条件に合えば、そのスクランブル鍵を消去する格納手段と、前記映像および／または音のデータを入力するとともに、前記スクランブル鍵発生手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記映像および／または音のデータをスクランブルするスクランブル手段と、前記スクランブル鍵によりスクランブルされた映像および／または音のデータと、そのスクランブル鍵との対応関係情報を生成する対応関係情報生成手段と、前記スクランブル手段からのスクランブルされた映像および／または音のデータ、および、前記対応関係情報生成手段からの対応関係情報の全部または一部を入力し、それらを所定の記録媒体に記録する記録手段とを備えたことを特徴とする録画装置である。

【００２１】

請求項１９の本発明は、請求項１５から１８のいずれかに記載の所定の記録媒体からの、請求項１５から１８のいずれかに記載の対応関係情報を入力し、その対応関係情報に基づいて、再生しようとするスクランブルされた映像および／または音のデータに対応するスクランブル鍵を特定し、請求項１５から１８のいずれかに記載の格納手段のなかの前記スクランブル鍵を検索して取得するスクランブル鍵取得手段と、前記所定の記録媒体からの、前記再生しようとするスクランブルされた映像および／または音のデータに対応する、前記スクランブルされた映像および／または音のデータを入力するとともに、前記スクランブル鍵取得手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記スクランブルされた映像および／または音のデータのスクランブルを解除するスクランブル解除手段とを備えたことを特徴とする再生装置である。

【００２２】

請求項２０の本発明は、映像および／または音のデータをスクランブルするためのスクランブル鍵を発生するスクランブル鍵発生手段と、前記スクランブル鍵発生手段が発生したスクランブル鍵を格納する格納手段と、前記映像および／または音のデータを入力するとともに、前記スクランブル鍵発生手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記映像および／または音のデータをスクランブルするスクランブル手段と、前記スクランブル鍵によりスクランブルされた映像および／または音のデータと、そのスクランブル鍵との対応関係情報を生成する対応関係情報生成手段と、前記スクランブル手段からのスクランブルされた映像および／または音のデータ、および、前記対応関係情報生成手段からの対応関係情報の全部または一部を入力し、それらを所定の記録媒体に記録する記録手段とを備えたことを特徴とする録画装置である。

【００２３】

請求項２２の本発明は、請求項２０または２１記載の所定の記録媒体からの、請求項２０または２１記載の対応関係情報を入力し、その対応関係情報に基づいて、再生しようとするスクランブルされた映像および／または音のデータに対応するスクランブル鍵を特定し、さらに、そのスクランブル鍵が所定の条件に合うかどうかを判定し、合致する場合は、そのスクランブル鍵を、請求項２０または

２１記載の格納手段から取り出し、合致しない場合は、そのスクランブル鍵を前記格納手段から取り出さないスクランブル鍵取得手段と、前記所定の記録媒体からの、前記再生しようとするスクランブルされた映像および／または音のデータに対応する、スクランブルされた映像および／または音のデータを入力するとともに、前記スクランブル鍵取得手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記スクランブルされた映像および／または音のデータのスクランブルを解除するスクランブル解除手段とを備えたことを特徴とする再生装置である。

【００２４】

【発明の実施の形態】

以下に、本発明の実施の形態を図面を参照して説明する。

【００２５】

（実施の形態１）

先ず、本発明の実施の形態１の録画装置および再生装置の構成を述べる。

【００２６】

図１に、本発明の実施の形態１の録画装置および再生装置のブロック図を示す。本発明の実施の形態１の録画装置は、第１鍵発生手段６と、記録スクランブル手段７と、第２鍵発生手段８と、ＫｃＦＩＦＯ９と、鍵暗号化手段１０と、対応関係情報生成手段１１と、ＭＵＸ１２から構成される。また、本発明の実施の形態１の再生装置は、第２ＤＭＵＸ１３と、暗号化鍵取得手段１４と、Ｋｃラッチ手段１５と、鍵解読手段１６と、再生デスクランブル手段１７から構成される。なお、図１には、受信復調手段１と、第１ＤＭＵＸ２と、ＥＭＭ解読手段３と、ＥＣＭ解読手段４と、放送デスクランブル手段５と、映像デコーダ１８と、音デコーダ１９も表示する。さらに、記録媒体としてのビデオテープ２０と、映像を表示し、音を出力するディスプレイ２１も表示する。

【００２７】

受信復調手段１は、放送局からの、デジィタルの映像データ、音データ、ＥＭＭ（個別情報）、ＥＣＭ（番組情報）および暗号化された放送スクランブル鍵Ｋｓを通信衛星を介して入力し、それらの全部または一部の信号波形を整形する手

段である。

【００２８】

なお、受信復調手段１が入力する映像データおよび音データは、放送スクランブル鍵Ｋｓによりスクランブルされたデータである。また、以下では、映像データと音データの両方を意味する場合、映像データおよび音データをＡＶデータとする。

【００２９】

また、受信復調手段１が入力するＥＭＭ（個別情報）は、後に説明するワーク鍵Ｋｗという鍵を生成するさいに必要となる情報である。

【００３０】

さらに、受信復調手段１が入力するＥＣＭ（番組情報）は、暗号化された放送スクランブル鍵Ｋｓを復元するさいに必要となる情報である。

【００３１】

さて、第１ＤＭＵＸ２は、受信復調手段１からの、波形整形された映像データ、音データ、ＥＭＭ、ＥＣＭおよび暗号化された放送スクランブル鍵Ｋｓを分離する手段であるとともに、放送デスクランブル手段５からの、デスクランブルされた映像データおよび音データを分離する手段である。また、第１ＤＭＵＸ２は、再生デスクランブル手段１７からの映像データおよび音データを分離する手段でもある。

【００３２】

ＥＭＭ解読手段３は、ユーザＩＤ鍵Ｋｍを入力するとともに、第１ＤＭＵＸ２からのＥＭＭを入力し、ユーザＩＤ鍵ＫｍでＥＭＭを解読してワーク鍵Ｋｗを生成する手段である。

【００３３】

ＥＣＭ解読手段４は、ＥＭＭ解読手段３からのワーク鍵Ｋｗを入力するとともに、第１ＤＭＵＸ２からのＥＣＭおよび暗号化された放送スクランブル鍵Ｋｓを入力し、ワーク鍵ＫｗでＥＣＭを解読して放送スクランブル鍵Ｋｓを復元する手段である。

【００３４】

放送デスクランブル手段５は、ＥＣＭ解読手段４からの放送スクランブル鍵Ｋｓを入力するとともに、第１ＤＭＵＸ２からの、スクランブルされたＡＶデータを入力し、放送スクランブル鍵Ｋｓで、スクランブルされたＡＶデータをデスクランブルする手段である。

【００３５】

第１鍵発生手段６は、放送デスクランブル手段５によってデスクランブルされたＡＶデータを、再度スクランブルするための記録スクランブル鍵Ｋｓｓを発生する手段である。

【００３６】

記録スクランブル手段７は、放送デスクランブル手段５からのＡＶデータを入力するとともに、第１鍵発生手段６からの記録スクランブル鍵Ｋｓｓを入力し、その記録スクランブル鍵ＫｓｓでＡＶデータをスクランブルする手段である。なお、以下では、記録スクランブル鍵Ｋｓｓによりスクランブルされたデータを Ｋｓｓ（ＡＶデータ）とする。

【００３７】

第２鍵発生手段８は、第１鍵発生手段６が発生した記録スクランブル鍵Ｋｓｓを暗号化するための暗号化鍵Ｋｃを発生する手段である。なお、第２鍵発生手段８は、毎日異なる暗号化鍵Ｋｃを発生するものとし、それら異なるＫｃをそれぞれＫｃ１、Ｋｃ２、Ｋｃ３、…とする。また、暗号化鍵Ｋｃ１、Ｋｃ２、Ｋｃ３、…それぞれは、１週間で廃棄されるものであるとする。

【００３８】

ＫｃＦＩＦＯ９は、第２鍵発生手段８からの暗号化鍵Ｋｃ１、Ｋｃ２、Ｋｃ３、…を入力し格納する手段であるとともに、タイマーを有していて、そのタイマーを利用して、入力後１週間経過した暗号化鍵Ｋｃを廃棄する、ファーストインファーストアウト機能を有する手段である。

【００３９】

鍵暗号化手段１０は、第１鍵発生手段６からの記録スクランブル鍵Ｋｓｓを入力するとともに、ＫｃＦＩＦＯ９からの暗号化鍵Ｋｃを入力し、その暗号化鍵Ｋｃで記録スクランブル鍵Ｋｓｓを暗号化する手段である。なお、以下では、暗号

化鍵Ｋｃにより暗号化された記録スクランブル鍵ＫｓｓをＫｃ（Ｋｓｓ）とする。

【００４０】

対応関係情報生成手段１１は、記録スクランブル鍵ＫｓｓによりスクランブルされたＡＶデータと、その記録スクランブル鍵Ｋｓｓを暗号化した暗号化鍵Ｋｃとを対応付けるための情報として、暗号化鍵Ｋｃ４が発生された日時の情報を生成する手段である。

【００４１】

ＭＵＸ１２は、記録スクランブル手段７からのＫｓｓ（ＡＶデータ）と、鍵暗号化手段１０からのＫｃ（Ｋｓｓ）と、対応関係情報生成手段１１からの日時情報とを入力し、それらをビデオテープ２０に記録する手段である。

【００４２】

第２ＤＭＵＸ１３は、ビデオテープ２０に記録された、Ｋｓｓ（ＡＶデータ）、Ｋｃ（Ｋｓｓ）および日時情報を入力し、それらを分離する手段である。

【００４３】

暗号化鍵取得手段１４は、第２ＤＭＵＸ１３からの日時情報を入力し、その日時情報に基づいて、再生しようとするＫｓｓ（ＡＶデータ）に対応する暗号化鍵Ｋｃを特定し、その特定した暗号化鍵ＫｃをＫｃＦＩＦＯ９のなかから取得する手段である。

【００４４】

Ｋｃラッチ手段１５は、暗号化鍵取得手段１４からの暗号化鍵Ｋｃを入力してラッチし、鍵解読手段１６に出力する手段である。

【００４５】

鍵解読手段１６は、第２ＤＭＵＸ１３からのＫｃ（Ｋｓｓ）を入力するとともに、Ｋｃラッチ手段１５からの暗号化鍵Ｋｃを入力し、その暗号化鍵ＫｃでＫｃ（Ｋｓｓ）を解読し、記録スクランブル鍵Ｋｓｓを復元する手段である。

【００４６】

再生デスクランブル手段１７は、第２ＤＭＵＸ１３からのＫｓｓ（ＡＶデータ）を入力するとともに、鍵解読手段１６からの記録スクランブル鍵Ｋｓｓを入力

し、その記録スクランブル鍵ＫｓｓでＫｓｓ（ＡＶデータ）をデスクランブルする手段である。

【００４７】

映像デコーダ１８は、第１ＤＭＵＸ２からの映像データを復号する手段である。

【００４８】

音デコーダ１９は、第１ＤＭＵＸ２からの音データを復号する手段である。

【００４９】

なお、請求項１の本発明の、スクランブル手段として記録スクランブル手段７、暗号化鍵発生手段として第２鍵発生手段８、格納手段としてＫｃＦＩＦＯ９、鍵暗号化手段として鍵暗号化手段１０、対応関係情報生成手段として対応関係情報生成手段１１、記録手段としてＭＵＸ１２を用いた。また、請求項６の本発明のスクランブル鍵発生手段として第１鍵発生手段６を、本実施の形態では用いた。さらに、請求項７の本発明の、暗号化鍵取得手段として暗号化鍵取得手段１４、鍵暗号化解読手段として鍵解読手段１６、スクランブル解除手段として再生デスクランブル手段１７を用いた。

【００５０】

次に、このような本発明の実施の形態１の録画装置の動作を述べる。

【００５１】

先ず、受信復調手段１は、放送局からの、デジィタルの映像データ、音データ、ＥＭＭ（個別情報）、ＥＣＭ（番組情報）および暗号化された放送スクランブル鍵Ｋｓを入力し、映像データおよび音データの信号波形の乱れを整形し、映像データ、音データ、ＥＭＭ、ＥＣＭおよび暗号化された放送スクランブル鍵Ｋｓを第１ＤＭＵＸ２に出力する。

【００５２】

その後、第１ＤＭＵＸ２は、受信復調手段１からの映像データ、音データ、ＥＭＭ、ＥＣＭおよび放送スクランブル鍵Ｋｓを入力して分離し、映像データおよび音データ（ＡＶデータ）を放送デスクランブル手段５に出力する。また、ＥＭＭをＥＭＭ解読手段３に出力し、ＥＣＭおよび暗号化された放送スクランブル鍵

ＫｓをＥＣＭ解読手段４に出力する。

【００５３】

次に、ＥＭＭ解読手段３は、ユーザＩＤ鍵Ｋｍを入力するとともに、第１ＤＭＵＸ２からのＥＭＭを入力し、ユーザＩＤ鍵ＫｍでＥＭＭを解読してワーク鍵Ｋｗを生成し、ＥＣＭ解読手段４に出力する。

【００５４】

さらに、ＥＣＭ解読手段４は、ＥＭＭ解読手段３からのワーク鍵Ｋｗを入力するとともに、第１ＤＭＵＸ２からの、ＥＣＭおよび暗号化された放送スクランブル鍵Ｋｓを入力し、ワーク鍵ＫｗでＥＣＭを解読して、暗号化された放送スクランブル鍵Ｋｓの暗号化を復元し、放送デスクランブル手段５に出力する。

そして、放送デスクランブル手段５は、ＥＣＭ解読手段４からの放送スクランブル鍵Ｋｓを入力するとともに、第１ＤＭＵＸ２からの、スクランブルされたＡＶデータを入力し、放送スクランブル鍵Ｋｓで、スクランブルされたＡＶデータをデスクランブルする。そして、放送デスクランブル手段５は、デスクランブルされたＡＶデータを第１ＤＭＵＸ２または記録スクランブル手段７に出力する。なお、放送デスクランブル手段５は、リアルタイムでＡＶデータを直接ディスプレイ２１に表示させる場合に第１ＤＭＵＸ２に出力し、ビデオテープ２０にＡＶデータを記録させる場合に記録スクランブル手段７に出力する。ただし、ビデオテープ２０に記録されるＡＶデータは、放送デスクランブル手段５からの、そのままのＡＶデータではなく、再度スクランブルされたデータである。

【００５５】

はじめに、放送デスクランブル手段５がＡＶデータを第１ＤＭＵＸ２に出力する場合について説明する。

【００５６】

その場合、第１ＤＭＵＸ２は、放送デスクランブル手段５からのＡＶデータ入力し、それを映像データと音データに分離して、映像データを映像デコーダ１８に出力し、音データを音デコーダ１９に出力する。その後、映像デコーダ１８および音デコーダ１９それぞれは、第１ＤＭＵＸ２からの映像データまたは音データを復号し、ディスプレイ２１に出力する。そして、ディスプレイ２１は、映像

を表示し音を出力する。

【００５７】

次に、放送デスクランブル手段５がＡＶデータを記録スクランブル手段７に出力する場合について説明する。つまり、上述したように、ビデオテープ２０にＡＶデータを記録する場合である。

【００５８】

先ず、記録スクランブル手段７は、放送デスクランブル手段５からの、デスクランブルされたＡＶデータを入力する。

【００５９】

そして、第１鍵発生手段６は、記録スクランブル手段７が入力したＡＶデータをスクランブルするための記録スクランブル鍵Ｋｓｓを発生し、記録スクランブル手段７および鍵暗号化手段１０に出力する。

【００６０】

次に、記録スクランブル手段７は、第１鍵発生手段６からの記録スクランブル鍵Ｋｓｓを入力し、その記録スクランブル鍵ＫｓｓでＡＶデータをスクランブルする。つまり、Ｋｓｓ（ＡＶデータ）を生成する。そして、Ｋｓｓ（ＡＶデータ）を対応関係情報生成手段１１およびＭＵＸ１２に出力する。

【００６１】

他方、第２鍵発生手段８は、第１鍵発生手段６が発生した記録スクランブル鍵Ｋｓｓを暗号化するための暗号化鍵Ｋｃを発生する。その第２鍵発生手段８が発生する暗号化鍵Ｋｃは毎日異なるものとする。ここでは、以下の説明の便宜上、録画装置が動作し始める日を１９９８年１月１日であるとし、記録時である本日をその日から３日後の１９９８年１月４日であるとし、図２の暗号化鍵Ｋｃリスト（ａ）に示すように、１月１日に発生された暗号化鍵ＫｃをＫｃ１、１月２日に発生された暗号化鍵ＫｃをＫｃ２、…、１月４日に発生された暗号化鍵ＫｃをＫｃ４とする。また、以下、同様にして暗号化鍵Ｋｃは発生されるものとする。なお、ことわりがない限り、以下、１月４日の録画装置の動作について説明する。

【００６２】

さて、ＫｃＦＩＦＯ９は、図２（ａ）のリストに示すように、１月１日から毎日一つづつの暗号化鍵Ｋｃを第２鍵発生手段８から既に入力して格納し、１月３日までに暗号化鍵Ｋｃ１、Ｋｃ２、Ｋｃ３を格納しておき、本日１月４日には、Ｋｃ４を入力して格納する。その格納は、常に最新の暗号化鍵Ｋｃが図２（ａ）のリストのトップの順位にくるように行われ、また、古いものは順次順位を下げるように行われる。なお、ＫｃＦＩＦＯ９は、格納した暗号化鍵Ｋｃ１、Ｋｃ２、…を、それぞれの格納から１週間経過した後に廃棄する。例えば、図２（ｂ）のリストに示すように、１月９日になると、Ｋｃ１、Ｋｃ２という暗号化鍵は廃棄され、ＫｃＦＩＦＯ９は、Ｋｃ９、Ｋｃ８、…、Ｋｃ４、Ｋｃ３という順序で７つの暗号化鍵を格納することになる。つまり、ＫｃＦＩＦＯ９が格納する暗号化鍵Ｋｃの数は７までである。

【００６３】

次に、鍵暗号化手段１０は、第１鍵発生手段６からの記録スクランブル鍵Ｋｓｓを入力するとともに、ＫｃＦＩＦＯ９を介して、第２鍵発生手段８が記録時である１月４日に発生した暗号化鍵Ｋｃ４を入力し、その暗号化鍵Ｋｃ４で記録スクランブル鍵Ｋｓｓを暗号化する。つまり、Ｋｃ４（Ｋｓｓ）を生成する。

【００６４】

そして、対応関係情報生成手段１１は、記録スクランブル手段７からのＫｓｓ（ＡＶデータ）と、鍵暗号化手段１０からのＫｃ４（Ｋｓｓ）とを入力し、その暗号化鍵Ｋｃ４と、その暗号化鍵Ｋｃ４で暗号化された記録スクランブル鍵Ｋｓｓによりスクランブルされたデータとを対応付けるための情報として、その暗号化鍵Ｋｃ４が発生された日時の情報を生成する。つまり、１月４日という日時情報を生成する。

【００６５】

その後、ＭＵＸ１２は、記録スクランブル手段７からのＫｓｓ（ＡＶデータ）と、鍵暗号化手段１０からのＫｃ４（Ｋｓｓ）と、対応関係情報生成手段１１からの１月４日という日時情報とを入力し、それらを１組としてビデオテープ２０に記録する。

【００６６】

このようにして、毎日、その日に発生された暗号化鍵Ｋｃｎ（ｎ＝１、２、…）に対応するＫｃｎ（Ｋｓｓ）と、Ｋｓｓ（ＡＶデータ）と、その日の日時情報とが１組となってビデオテープ２０に記録される。

【００６７】

次に、本発明の実施の形態１の再生装置の動作を述べる。

【００６８】

つまり、録画装置によってビデオテープ２０に記録されたＫｓｓ（ＡＶデータ）を再生する場合について説明する。

【００６９】

以下の説明の便宜上、再生装置がビデオテープ２０のＫｓｓ（ＡＶデータ）を再生する日を１月９日であるとする。そして、再生装置は、１月１日にビデオテープ２０に記録されたＫｓｓ（ＡＶデータ）と、１月３日にビデオテープ２０に記録されたＫｓｓ（ＡＶデータ）とを再生しようとするものとする。

【００７０】

はじめに、再生装置が１月１日にビデオテープ２０に記録されたＫｓｓ（ＡＶデータ）を再生しようとする場合について説明する。

【００７１】

先ず、第２ＤＭＵＸ１３は、ビデオテープ２０からの、１月１日に記録されたＫｓｓ（ＡＶデータ）と、Ｋｃ１（Ｋｓｓ）と、１月１日という日時情報とを入力し、それらを分離し、１月１日という日時情報を暗号化鍵取得手段１４に出力する。

【００７２】

そして、暗号化鍵取得手段１４は、その１月１日という日時情報を入力し、その日時情報に基づいて、暗号化鍵Ｋｃ１を特定し、ＫｃＦＩＦＯ９が格納している、図２（ｂ）のリストのなかから暗号化鍵Ｋｃ１を検索する。しかしながら、その暗号化鍵Ｋｃ１は、発生から一週間以上経過しているので、ＫｃＦＩＦＯ９により廃棄されており、図２（ｂ）のリストのなかには存在しない。したがって、暗号化鍵取得手段１４は、暗号化鍵Ｋｃ１を取得することができない。その結果、再生デスクランブル手段１７は、その暗号化鍵Ｋｃ１を間接的に用いてデス

クランブルする必要がある、１月１日に記録されたＫｓｓ（ＡＶデータ）をデスクランブルすることができなくなり、そのＡＶデータがディスプレイ２１に出力されても、解読不能なため、ディスプレイ２１は、ＡＶデータ本来の映像および音を出力することができない。

【００７３】

次に、再生装置が１月３日にビデオテープ２０に記録されたＫｓｓ（ＡＶデータ）を再生しようとする場合について説明する。

【００７４】

先ず、第２ＤＭＵＸ１３は、ビデオテープ２０からの、１月３日に記録されたＫｓｓ（ＡＶデータ）と、Ｋｃ３（Ｋｓｓ）と、１月３日という日時情報とを入力し、それらを分離し、１月３日という日時情報を暗号化鍵取得手段１４に出力する。

【００７５】

次に、暗号化鍵取得手段１４は、その１月３日という日時情報を入力し、その日時情報に基づいて、暗号化鍵Ｋｃ３を特定し、ＫｃＦＩＦＯ９が格納している、図２（ｂ）のリストのなかから暗号化鍵Ｋｃ３を検索してその暗号化鍵Ｋｃ３を取得し、それをＫｃラッチ手段１５に出力する。

【００７６】

その後、Ｋｃラッチ手段１５は、暗号化鍵Ｋｃ３を入力し、鍵解読手段１６に出力する。また、第２ＤＭＵＸ１３は、Ｋｃ３（Ｋｓｓ）を鍵解読手段１６に出力する。

【００７７】

そして、鍵解読手段１６は、第２ＤＭＵＸ１３からのＫｃ３（Ｋｓｓ）を入力するとともに、Ｋｃラッチ手段１５からの暗号化鍵Ｋｃ３を入力し、その暗号化鍵Ｋｃ３でＫｃ３（Ｋｓｓ）を解読し、記録スクランブル鍵Ｋｓｓを復元して、その記録スクランブル鍵Ｋｓｓを再生デスクランブル手段１７に出力する。また、第２ＤＭＵＸ１３は、Ｋｓｓ（ＡＶデータ）を鍵解読手段１６に出力する。

【００７８】

次に、再生デスクランブル手段１７は、第２ＤＭＵＸ１３からのＫｓｓ（ＡＶ

データ）を入力するとともに、鍵解読手段１６からの記録スクランブル鍵Ｋｓｓを入力し、その記録スクランブル鍵ＫｓｓでＫｓｓ（ＡＶデータ）をデスクランブルして、そのデスクランブルされたＡＶデータを第１ＤＭＵＸ２に出力する。

【００７９】

そして、第１ＤＭＵＸ２は、再生デスクランブル手段１７からのＡＶデータを入力し、それを映像データと音データに分離して、映像データを映像デコーダ１８に出力し、音データを音デコーダ１９に出力する。その後、映像デコーダ１８および音デコーダ１９それぞれは、第１ＤＭＵＸ２からの映像データまたは音データを復号し、ディスプレイ２１に出力する。そして、ディスプレイ２１は、映像を表示し音を出力する。

【００８０】

このようにして、ビデオテープ２０に記録されたＫｓｓ（ＡＶデータ）それぞれは、記録されてから１週間以内でないと、最終的に、本来の映像および音声として再生されない。

【００８１】

なお、上述した実施の形態１では、ビデオテープ２０に記録されたＫｓｓ（ＡＶデータ）それぞれは、記録されてから１週間以内であれば再生されるとしたが、１週間以内というような期間の制限ではなく、Ｋｓｓ（ＡＶデータ）それぞれの再生回数を、例えば１回や３回というように制限して、その制限再生回数内でないと、再生されないとしてもよい。つまり、図３に示すように、本発明の再生装置がカウンタ２２を備え、そのカウンタ２２が各Ｋｓｓ（ＡＶデータ）の再生回数をチェックし、例えば１回や３回というような制限された再生回数に達した場合、ＫｃＦＩＦＯ９が、そのＫｓｓ（ＡＶデータ）に対応する暗号化鍵Ｋｃを廃棄するとしてもよい。また、上述した１週間以内というような期間の制限と再生回数の制限を併用するとしてもよい。

【００８２】

また、上述した実施の形態１では、ＫｃＦＩＦＯ９は、格納した暗号化鍵Ｋｃを１週間経過した後に廃棄するとした。しかし、ＫｃＦＩＦＯ９は、格納した暗号化鍵Ｋｃを１週間経過しても廃棄せずに、格納したままにしておき、暗号化鍵

取得手段１４が、Ｋｓｓ（ＡＶデータ）を再生しようとする日が暗号化鍵Ｋｃの発生から１週間以内か否かを判断して、または、制限回数内か否かを判断して、１週間以内または制限回数内以内であれば、再生しようとするＫｓｓ（ＡＶデータ）に対応する暗号化鍵ＫｃをＫｃＦＩＦＯ９から取得できるとしてもよい。したがって、この場合、請求項８の本発明では、スクランブル手段として記録スクランブル手段７、暗号化鍵発生手段として第２鍵発生手段８、格納手段としてＫｃＦＩＦＯ９、鍵暗号化手段として鍵暗号化手段１０、対応関係情報生成手段として対応関係情報生成手段１１、記録手段としてＭＵＸ１２がそれぞれ該当することになる。また、請求項１２の本発明では、暗号化鍵取得手段として暗号化鍵取得手段１４、鍵暗号化解読手段として鍵解読手段１６、スクランブル解除手段として再生デスクランブル手段１７がそれぞれ該当することになる。

【００８３】

また、上述した実施の形態１では、第１鍵発生手段６は、記録スクランブル手段７が入力したＡＶデータをスクランブルするための記録スクランブル鍵Ｋｓｓを発生するとした。しかし、本発明の録画装置は、図４に示すように、第１鍵発生手段６を備えず、記録スクランブル手段７は、放送局から送られてくる放送スクランブル鍵Ｋｓを、放送デスクランブル手段５を介して入力し、その放送スクランブル鍵Ｋｓで、または、その放送スクランブル鍵Ｋｓを加工したもので、ＡＶデータをスクランブルするとしてもよい。その場合、鍵暗号化手段１０は、記録スクランブル手段７から、放送スクランブル鍵Ｋｓ、または、その放送スクランブル鍵Ｋｓを加工したものを入力し、それを暗号化鍵Ｋｃで暗号化する。

【００８４】

また、上述した実施の形態１では、記録スクランブル手段７は、第１鍵発生手段６からの記録スクランブル鍵ＫｓｓでＡＶデータをスクランブルするとした。しかし、本発明の録画装置は、図５に示すように、第１鍵発生手段６、鍵暗号化手段１０を備えず、記録スクランブル手段７は、第２鍵発生手段８からの暗号化鍵ＫｃをＫｃＦＩＦＯ９を介して入力し、その暗号化鍵Ｋｃを記録スクランブル鍵Ｋｃとして使用し、その記録スクランブル鍵Ｋｃにより、ＡＶデータをスクランブルするとしてもよい。この場合、ビデオテープ２０には、記録スクランブル

鍵Ｋｃによりスクランブルされたａｖデータ、つまり、Ｋｃ（ＡＶデータ）と、記録スクランブル鍵Ｋｃとが記録される。またその場合、本発明の再生装置は、図５に示すように、鍵解読手段１６を備えないことになる。したがって、Ｋｃ（ＡＶデータ）を再生しようとする場合、スクランブル鍵取得手段２３は、対応する記録スクランブル鍵Ｋｃを特定し、それをＫｃＦＩＦＯ９のなかから取得する。そして、再生デスクランブル手段１７は、ビデオテープ２０からのＫｃ（ＡＶデータ）を第２ＤＭＵＸ１３を介して入力するとともに、スクランブル鍵取得手段２３からの記録スクランブル鍵ＫｃをＫｃラッチ手段１５を介して入力し、その記録スクランブル鍵ＫｃでＫｃ（ＡＶデータ）をデスクランブルする。そのため、この場合、つまり、請求項１５および２０の本発明では、スクランブル鍵発生手段として第２鍵発生手段８、格納手段としてＫｃＦＩＦＯ９、スクランブル手段として記録スクランブル手段７、対応関係情報生成手段として対応関係情報生成手段１１、記録手段として第１ＤＭＵＸ２がそれぞれ該当することになる。また、請求項１９および２２の本発明では、スクランブル鍵取得手段としてスクランブル鍵取得手段２３、スクランブル解除手段として再生デスクランブル手段１７がそれぞれ該当することになる。

【００８５】

また、上述した実施の形態１の録画装置は、図６に示すように、課金手段２４を備え、ビデオテープ２０にＫｓｓ（ＡＶデータ）を記録するさい、その記録に対する所定の課金をユーザに課し、あらかじめユーザから所定の料金が放送局等に支払われた場合、もしくは、少なくとも記録するさいに所定の料金が支払われた場合のみ、Ｋｓｓ（ＡＶデータ）はビデオテープ２０に記録されるとしてもよい。また、課金手段２４は、図６に示す位置に配置されなくとも、鍵暗号化手段１０とＭＵＸ１２との間に配置されるとしてもよい。要するに、課金手段２４は、ビデオテープ２０にＫｓｓ（ＡＶデータ）を記録するさい、その記録に対する所定の課金をユーザに課すものでありさえすればよく、配置場所はどの場所であってもよい。

【００８６】

また、上述した実施の形態１では、暗号化鍵Ｋｃそれぞれは、発生から１週間

経過すると廃棄されるとしたが、廃棄される日時は、発生から１週間経過後に限定することはなく、１日経過後であっても、３日経過後であっても、または、１２時間経過後であってもよい。要するに、暗号化鍵Ｋｃそれぞれは、発生から所定の期間経過すると廃棄されさえすればよい。

【００８７】

また、上述した実施の形態１では、第２鍵発生手段８は、毎日、１つづつ異なる暗号化鍵Ｋｃを発生するとしたが、第２鍵発生手段８は、同じ日であっても、数時間毎に異なる暗号化鍵Ｋｃを発生するとしてもよい。さらに、ビデオテープ２０に所定の番組のＫｓｓ（ＡＶデータ）を記録する毎に暗号化鍵Ｋｃを発生するとしてもよい。つまり、一回の録画開始からその録画の終了毎に、その都度、暗号化鍵Ｋｃを発生するとしてもよい。要するに、第２鍵発生手段８は、記録しようとするＫｓｓ（ＡＶデータ）の記録スクランブル鍵Ｋｓｓを暗号化するための暗号化鍵Ｋｃを発生しさえすればよい。

【００８８】

また、上述した実施の形態１では、本発明の対応関係情報として、暗号化鍵Ｋｃが発生されたさいの日時情報を用いたが、本発明の対応関係情報は、記録スクランブル手段７がＡＶデータを入力した日時、記録スクランブル手段７が記録スクランブル鍵ＫｓｓでＡＶデータをスクランブルした日時、第２鍵発生手段８が暗号化鍵Ｋｃを発生した日時、ＫｃＦＩＦＯ９が暗号化鍵Ｋｃを格納した日時、鍵暗号化手段１０が暗号化鍵Ｋｃで記録スクランブル鍵Ｋｓｓを暗号化した日時、または、ＭＵＸ１２がビデオテープ２０にＫｓｓ（ＡＶデータ）を記録した日時の情報であってもよい。もしくは、上述した暗号化鍵Ｋｃが発生されたさいの日時や、記録スクランブル手段７がＡＶデータを入力した日時等と、ＡＶデータを再生しようとする日時との情報であってもよい。その場合、図２の暗号化鍵Ｋｃリストの各暗号化鍵Ｋｃが毎日順位を下げることに基づいて、また、２つの日時の差が考慮されて、暗号化鍵Ｋｃが取得されることになる。または、本発明の対応関係情報は、上述した暗号化鍵Ｋｃが発生されたさいの日時や、記録スクランブル手段７がＡＶデータを入力した日時等と、ＡＶデータを再生しようとする日時とに基づき、また、図２の暗号化鍵Ｋｃリストの各暗号化鍵Ｋｃが毎日順位

を下げることが考慮された、図２の暗号化鍵Ｋｃリストの番号情報等であってもよい。

【００８９】

また、上述した実施の形態１では、記録媒体としてのビデオテープ２０を用いたが、記録媒体は、ビデオテープ２０に限らず、ハードディスクであってもよい。

【００９０】

また、上述した実施の形態１では、第１鍵発生手段６はＡＶデータをスクランブルするための記録スクランブル鍵Ｋｓｓを発生するが、その記録スクランブル鍵Ｋｓｓは、簡単に解読することができないように、例えば数十秒などの短い期間で更新されるとしてもよい。

【００９１】

さらに、上述した録画装置または再生装置は、暗号化鍵Ｋｃの発生から例えば１週間という所定の期間を経過するなどして、その暗号化鍵Ｋｃが廃棄されたり、使用不可になる前に、その暗号化鍵Ｋｃに対応するＫｓｓ（ＡＶデータ）が一度も再生されていない場合、その旨の情報をユーザに通知する手段を備えてもよい。

【００９２】

【発明の効果】

以上説明したところから明らかなように、本発明は、ＡＶデータを記録媒体に記録し、そのＡＶデータの有効再生期間や有効再生回数の制限を遵守する録画装置および再生装置を提供することができる。

【図面の簡単な説明】

【図１】

本発明の実施の形態１の録画装置および再生装置のブロック図

【図２】

本発明の実施の形態１の録画装置および再生装置に使用される暗号化鍵Ｋｃリストの一例を示す図

【図３】

図１とは異なる本発明の録画装置および再生装置のブロック図

【図４】

図１または３とは異なる本発明の録画装置および再生装置のブロック図

【図５】

図１、３または４とは異なる本発明の録画装置および再生装置のブロック図

【図６】

図１、３、４または５とは異なる本発明の録画装置および再生装置のブロック図

【図７】

従来の録画再生装置のブロック図

【符号の説明】

１　受信復調手段
２　第１ＤＭＵＸ
３　ＥＭＭ解読手段
４　ＥＣＭ解読手段
５　放送デスクランブル手段
６　第１鍵発生手段
７　記録スクランブル手段
８　第２鍵発生手段
９　ＫｃＦＩＦＯ
１０　鍵暗号化手段
１１　対応関係情報生成手段
１２　ＭＵＸ
１３　第２ＤＭＵＸ
１４　暗号化鍵取得手段
１５　Ｋｃラッチ手段
１６　鍵解読手段
１７　再生デスクランブル手段
１８　映像デコーダ

１９　音デコーダ

２０　ビデオテープ

２１　ディスプレイ

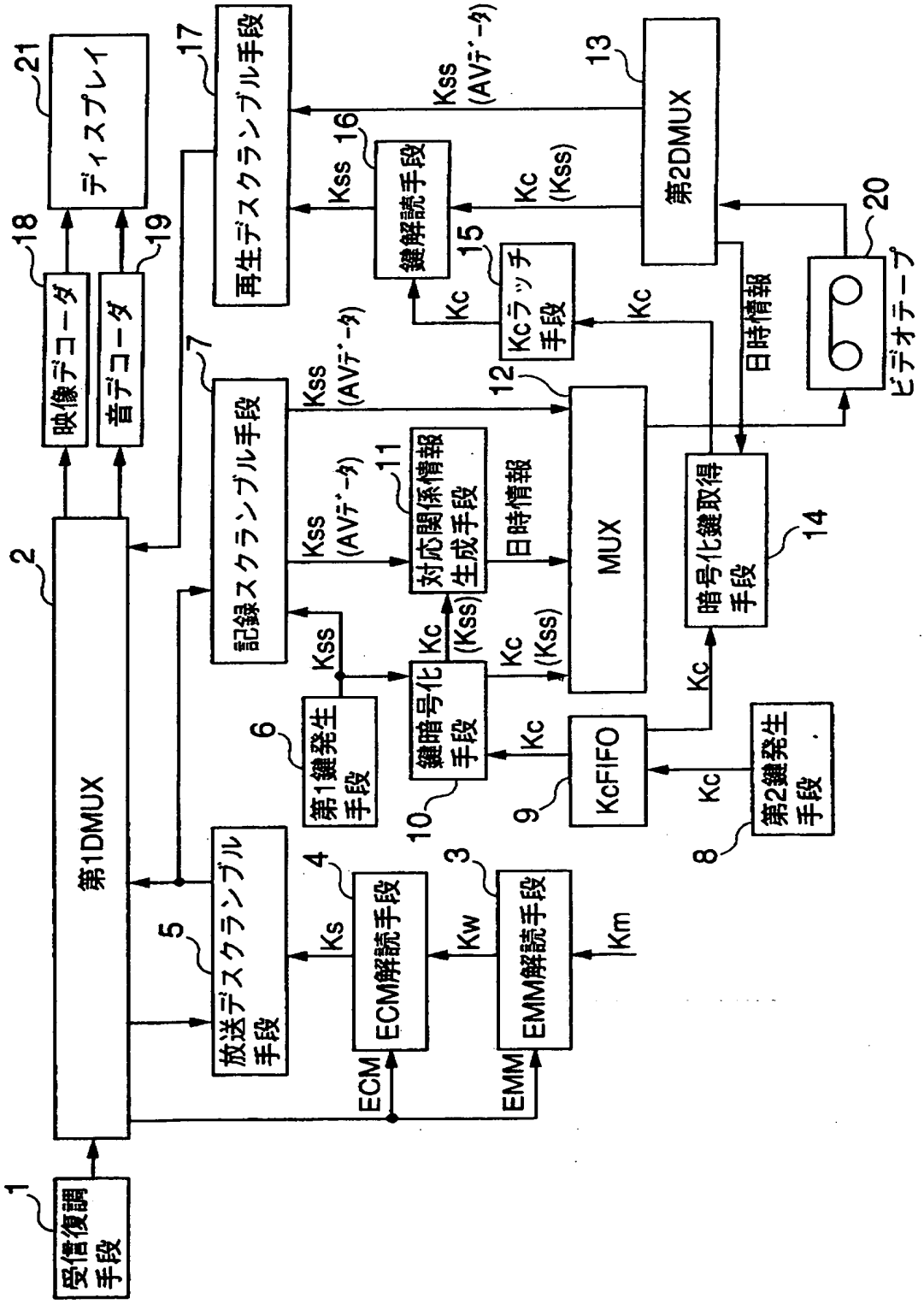
２２　カウンタ

２３　スクランブル鍵取得手段

２４　課金手段

【書類名】　図面

【図１】


受信復調手段
1
第1DMUX
2
放送デスクランブル手段
5
ECM解読手段
4
EMM解読手段
3
第1鍵発生手段
6
KcFIFO
9
第2鍵発生手段
8
鍵暗号化手段
10
記録スクランブル手段
7
対応関係情報生成手段
11
MUX
12
暗号化鍵取得手段
14
第2DMUX
13
再生デスクランブル手段
17
鍵解読手段
16
Kcラッチ手段
15
ディスプレイ
21
映像デコーダ
18
音デコーダ
19
ビデオテープ
20
日時情報
Ks
Kw
Km
ECM
EMM
Kc
Kss
(Kss)
Kss (AVデータ)

暗号化鍵 Kc リスト

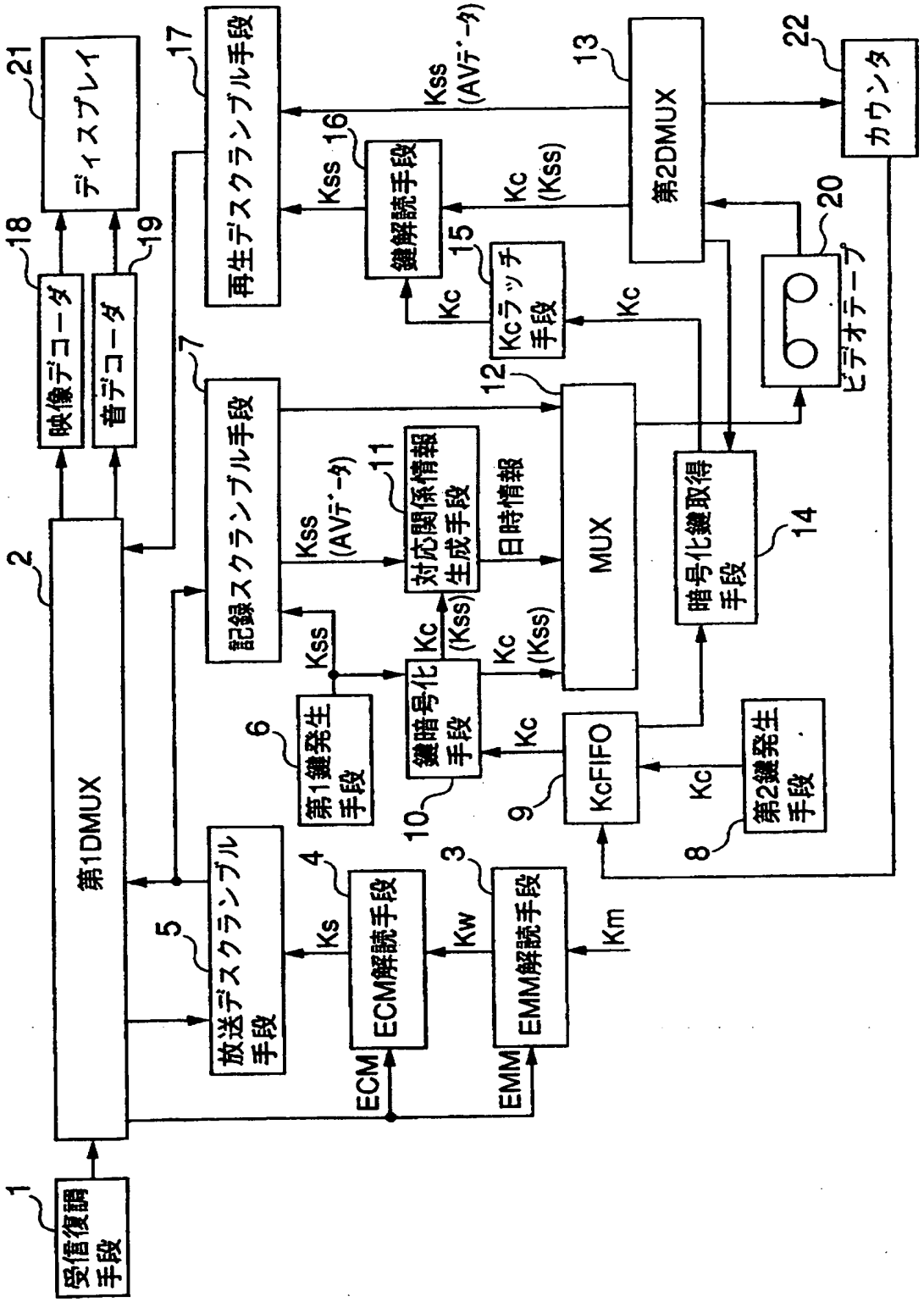
(a)　1月 4日 現在

No.	暗号化鍵	鍵発生日
1	Kc 4	1月 4日
2	Kc 3	1月 3日
3	Kc 2	1月 2日
4	Kc 1	1月 1日
5		
6		
7		

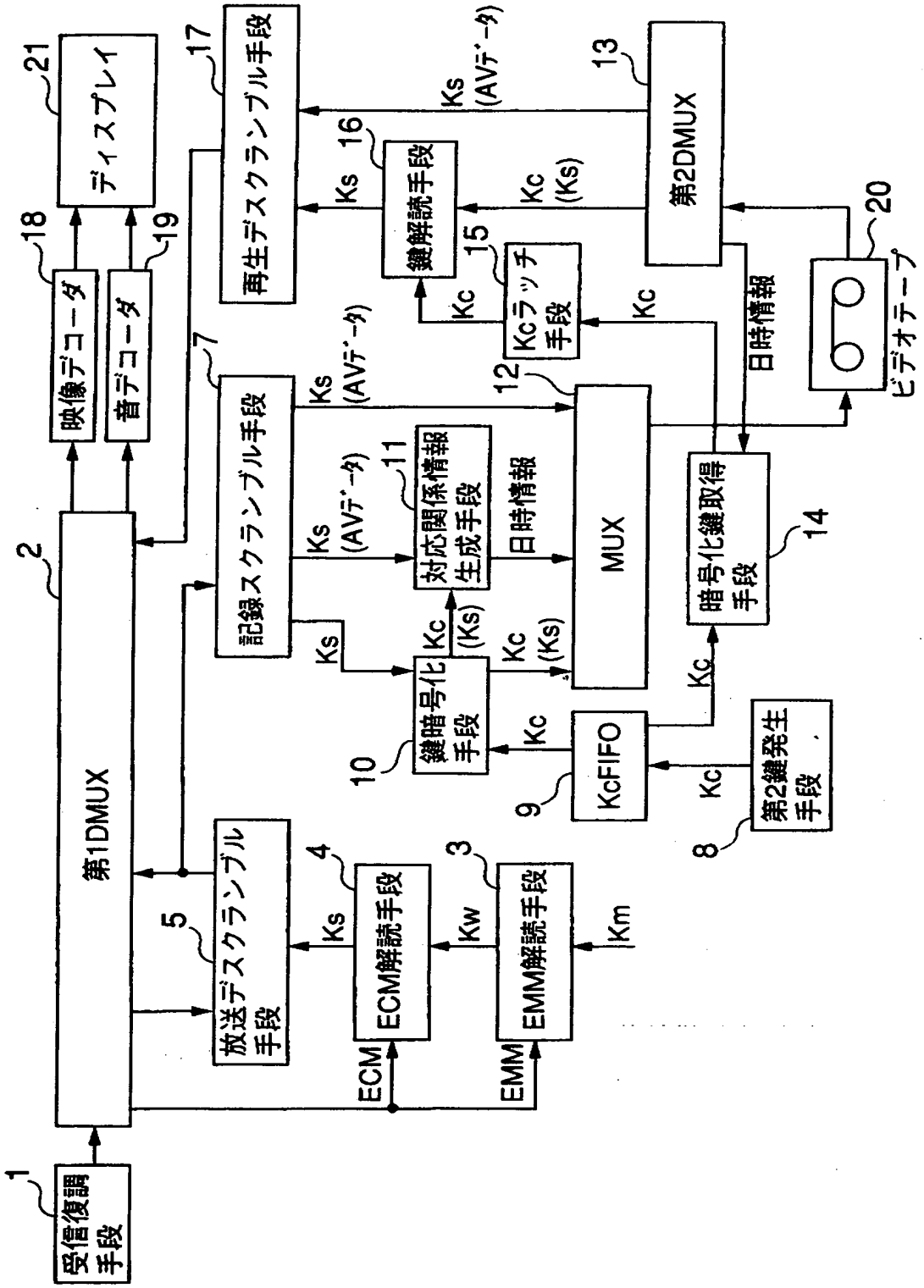
(b)　1月 9日 現在

No.	暗号化鍵	鍵発生日
1	Kc 9	1月 9日
2	Kc 8	1月 8日
3	Kc 7	1月 7日
4	Kc 6	1月 6日
5	Kc 5	1月 5日
6	Kc 4	1月 4日
7	Kc 3	1月 3日

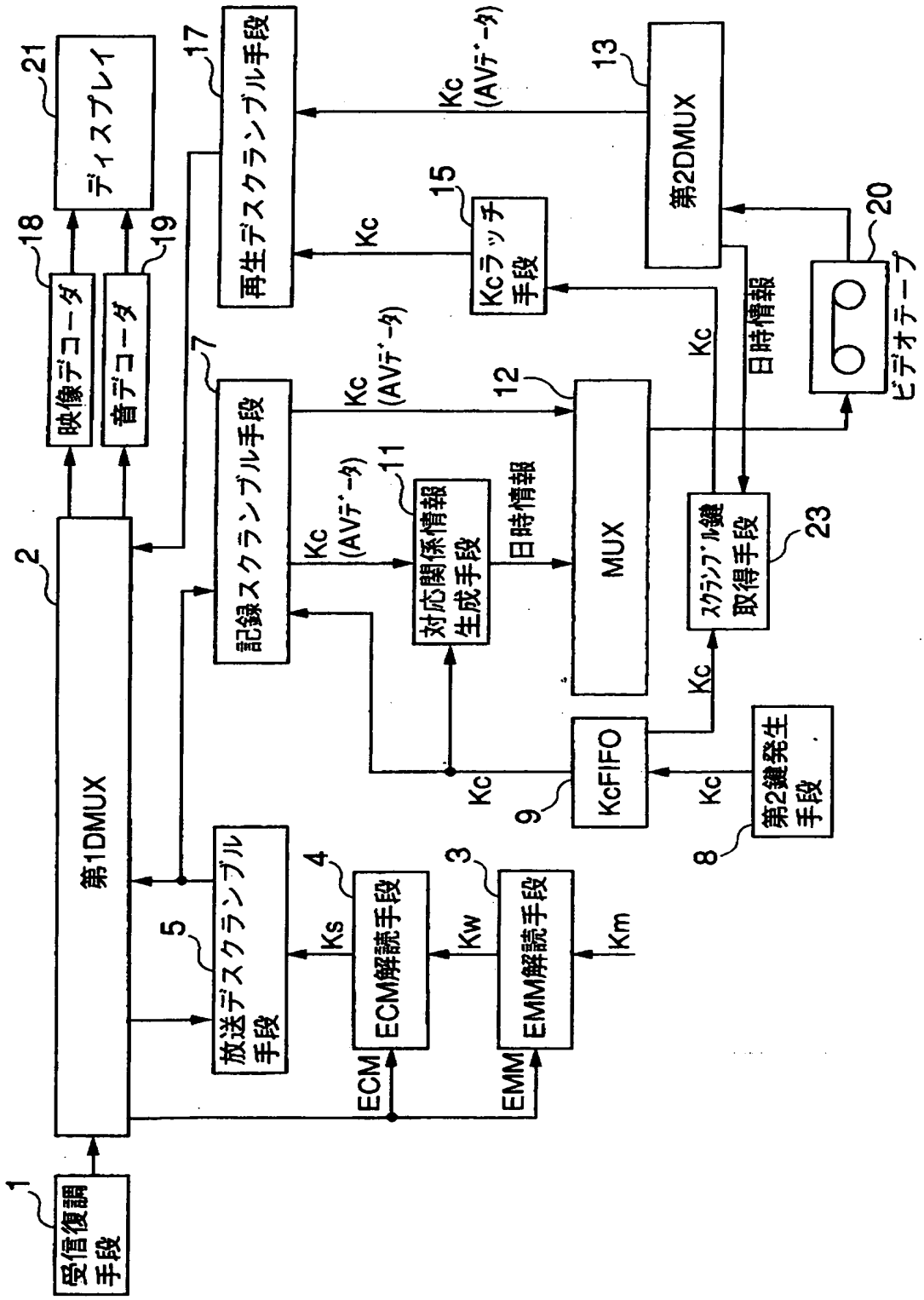
【図３】


受信復調手段
1
第1DMUX
2
放送デスクランブル手段
5
ECM解読手段
4
EMM解読手段
3
ECM
EMM
Ks
Kw
Km
第1鍵発生手段
6
鍵暗号化手段
10
KcFIFO
9
第2鍵発生手段
8
Kc
Kss
記録スクランブル手段
7
対応関係情報生成手段
11
日時情報
MUX
12
暗号化鍵取得手段
14
再生デスクランブル手段
17
鍵解読手段
16
Kcラッチ手段
15
第2DMUX
13
カウンタ
22
ビデオテープ
20
映像デコーダ
18
音デコーダ
19
ディスプレイ
21
Kss (AVデータ)
Kc (Kss)

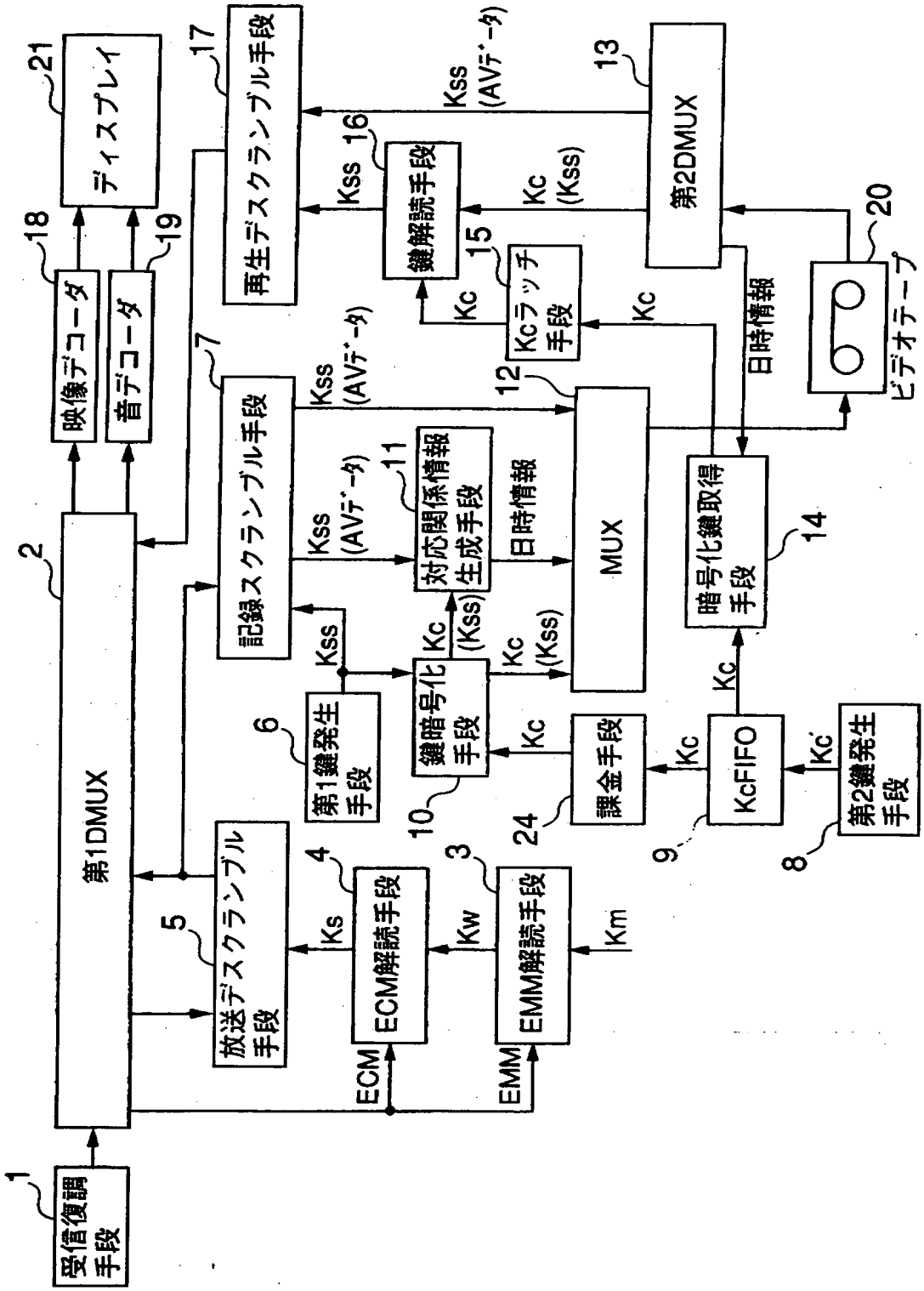
【図４】


1
受信復調手段
2
第1DMUX
3
EMM解読手段
4
ECM解読手段
5
放送デスクランブル手段
7
記録スクランブル手段
8
第2鍵発生手段
9
KcFIFO
10
鍵暗号化手段
11
対応関係情報生成手段
12
MUX
13
第2DMUX
14
暗号化鍵取得手段
15
Kcラッチ手段
16
鍵解読手段
17
再生デスクランブル手段
18
映像デコーダ
19
音デコーダ
20
ビデオテープ
21
ディスプレイ
ECM
EMM
Km
Kw
Ks
Kc
(Ks)
(AVデータ)
日時情報

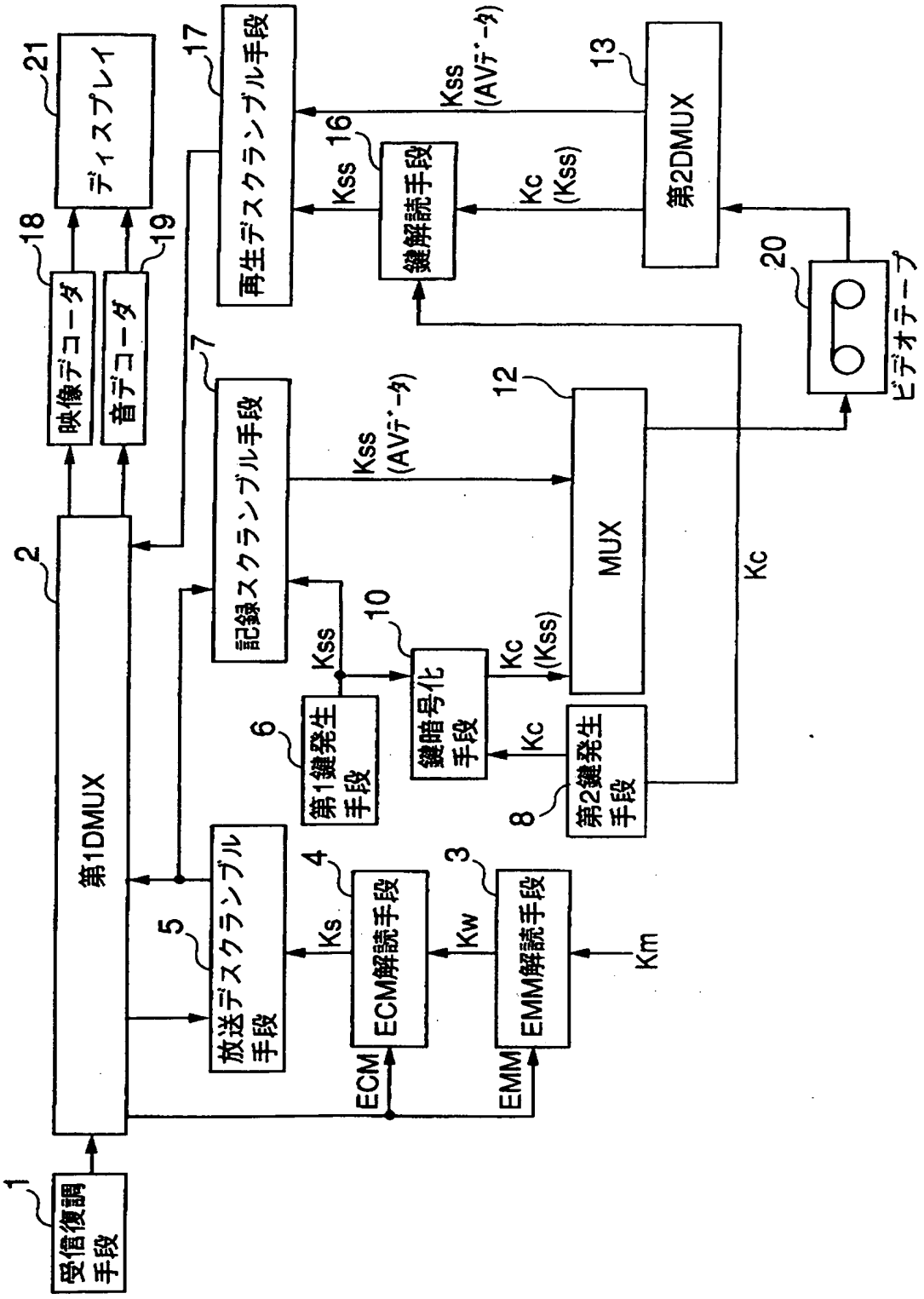
【図５】


受信復調手段
1
第1DMUX
2
放送デスクランブル手段
5
ECM解読手段
4
Ks
EMM解読手段
3
Kw
Km
ECM
EMM
記録スクランブル手段
7
対応関係情報生成手段
11
日時情報
MUX
12
KcFIFO
9
第2鍵発生手段
8
スクランブル鍵取得手段
23
Kcラッチ手段
15
再生デスクランブル手段
17
第2DMUX
13
ビデオテープ
20
ディスプレイ
21
映像デコーダ
18
音デコーダ
19
Kc
(AVデータ)
日時情報

【図６】


受信復調手段
1
第1DMUX
2
放送デスクランブル手段
5
記録スクランブル手段
7
再生デスクランブル手段
17
ECM解読手段
4
EMM解読手段
3
第1鍵発生手段
6
鍵暗号化手段
10
課金手段
24
KcFIFO
9
第2鍵発生手段
8
暗号化鍵取得手段
14
MUX
12
対応関係情報生成手段
11
鍵解読手段
16
Kcラッチ手段
15
第2DMUX
13
映像デコーダ
18
音デコーダ
19
ディスプレイ
21
ビデオテープ
20
日時情報
Ks
Kw
Km
Kc
Kc'
Kss
(Kss)
Kss (AVデータ)
Kc (Kss)
ECM
EMM

【図７】


受信復調手段
1
第1DMUX
2
放送デスクランブル手段
5
ECM解読手段
4
EMM解読手段
3
Ks
Kw
Km
ECM
EMM
第1鍵発生手段
6
第2鍵発生手段
8
鍵暗号化手段
10
Kc
(Kss)
記録スクランブル手段
7
Kss
(AVデータ)
MUX
12
第2DMUX
13
鍵解読手段
16
再生デスクランブル手段
17
Kss
(AVデータ)
ディスプレイ
21
映像デコーダ
18
音デコーダ
19
ビデオテープ
20

【書類名】　要約書

【要約】

【課題】従来の録画再生装置は、ＡＶデータを記録媒体に記録すると、そのＡＶデータの有効再生期間や有効再生回数の制限を守らないという課題があった。

【解決手段】スクランブル鍵ＫｓｓでＡＶデータをスクランブルする記録スクランブル手段７と、スクランブル鍵Ｋｓｓを暗号化するための暗号化鍵Ｋｃを発生する第２鍵発生手段８と、第２鍵発生手段８からの暗号化鍵Ｋｃを格納し、その後、その暗号化鍵Ｋｃが所定の条件に合えば、その暗号化鍵Ｋｃを消去するＫｃＦＩＦＯ９と、暗号化鍵Ｋｃでスクランブル鍵Ｋｓｓを暗号化する鍵暗号化手段１０と、暗号化鍵Ｋｃが発生された日時の情報を生成する対応関係情報生成手段１１と、スクランブルされた映像および／または音のデータ、暗号化されたスクランブル鍵Ｋｓｓ、および、日時情報を入力し、それらをビデオテープ２０に記録するＭＵＸ１２とを備える。

【選択図】　図１

出証特平１１－３０１７３９３

【書類名】　職権訂正データ
【訂正書類】　特許願

＜認定情報・付加情報＞
【特許出願人】
【識別番号】　000005821
【住所又は居所】　大阪府門真市大字門真１００６番地
【氏名又は名称】　松下電器産業株式会社
【代理人】　申請人
【識別番号】　100092794
【住所又は居所】　大阪市淀川区宮原５丁目１番３号　新大阪生島ビル　松田特許事務所
【氏名又は名称】　松田　正道

出　願　人　履　歴　情　報

識別番号　　〔０００００５８２１〕

１．変更年月日　　１９９０年　８月２８日
［変更理由］　新規登録
住　所　　大阪府門真市大字門真１００６番地
氏　名　　松下電器産業株式会社